100

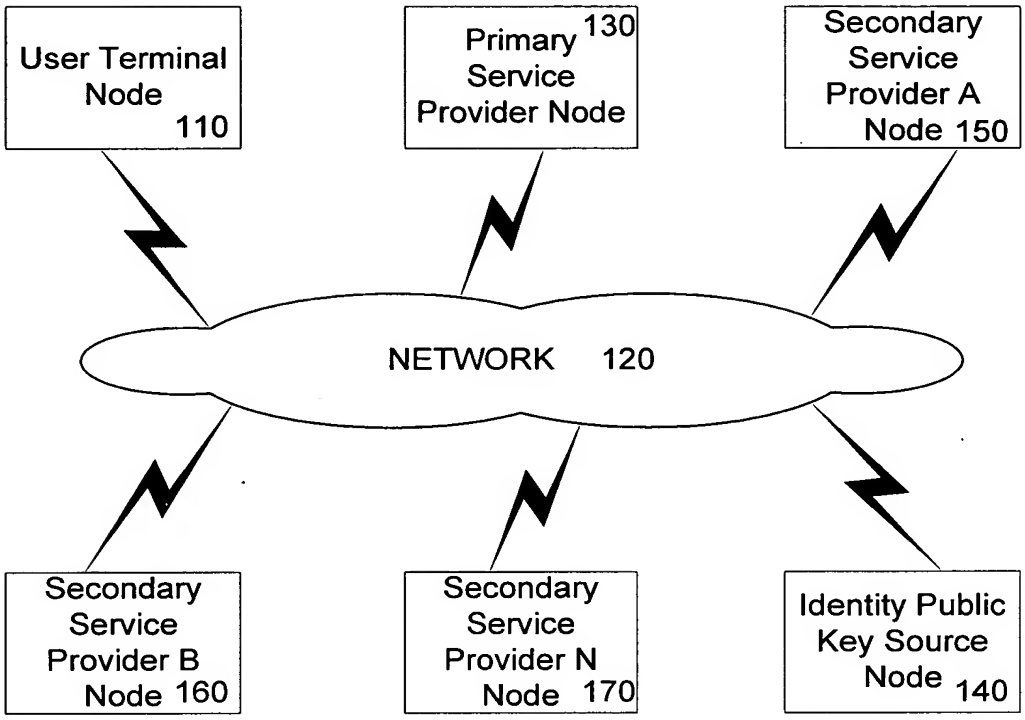
User Terminal Node 110
Primary Service Provider Node 130
Secondary Service Provider A Node 150
NETWORK 120
Secondary Service Provider B Node 160
Secondary Service Provider N Node 170
Identity Public Key Source Node 140

Fig. 1

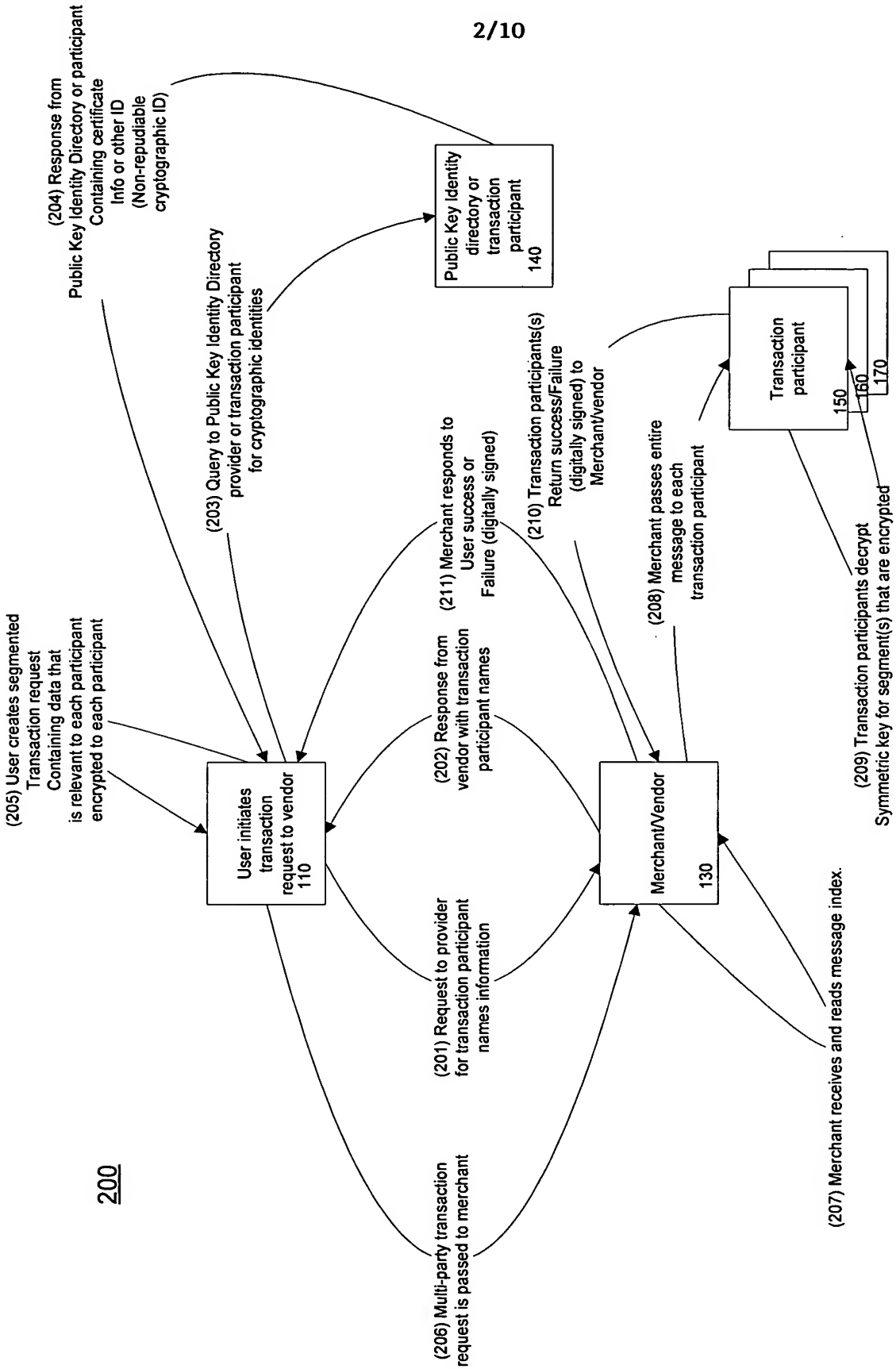
200
(205) User creates segmented Transaction request Containing data that is relevant to each participant encrypted to each participant
(204) Response from Public Key Identity Directory or participant Containing certificate Info or other ID (Non-repudiable cryptographic ID)
(203) Query to Public Key Identity Directory provider or transaction participant for cryptographic identities
Public Key Identity directory or transaction participant 140
User initiates transaction request to vendor 110
(202) Response from vendor with transaction participant names
(211) Merchant responds to User success or Failure (digitally signed)
(210) Transaction participants(s) Return success/Failure (digitally signed) to Merchant/vendor
(208) Merchant passes entire message to each transaction participant
Transaction participant 150 160 170
(201) Request to provider for transaction participant names information
Merchant/Vendor 130
(209) Transaction participants decrypt Symmetric key for segment(s) that are encrypted to their identities, decrypt data and enters transaction element for merchant/vendor
(206) Multi-party transaction request is passed to merchant
(207) Merchant receives and reads message index.

Fig. 2

300

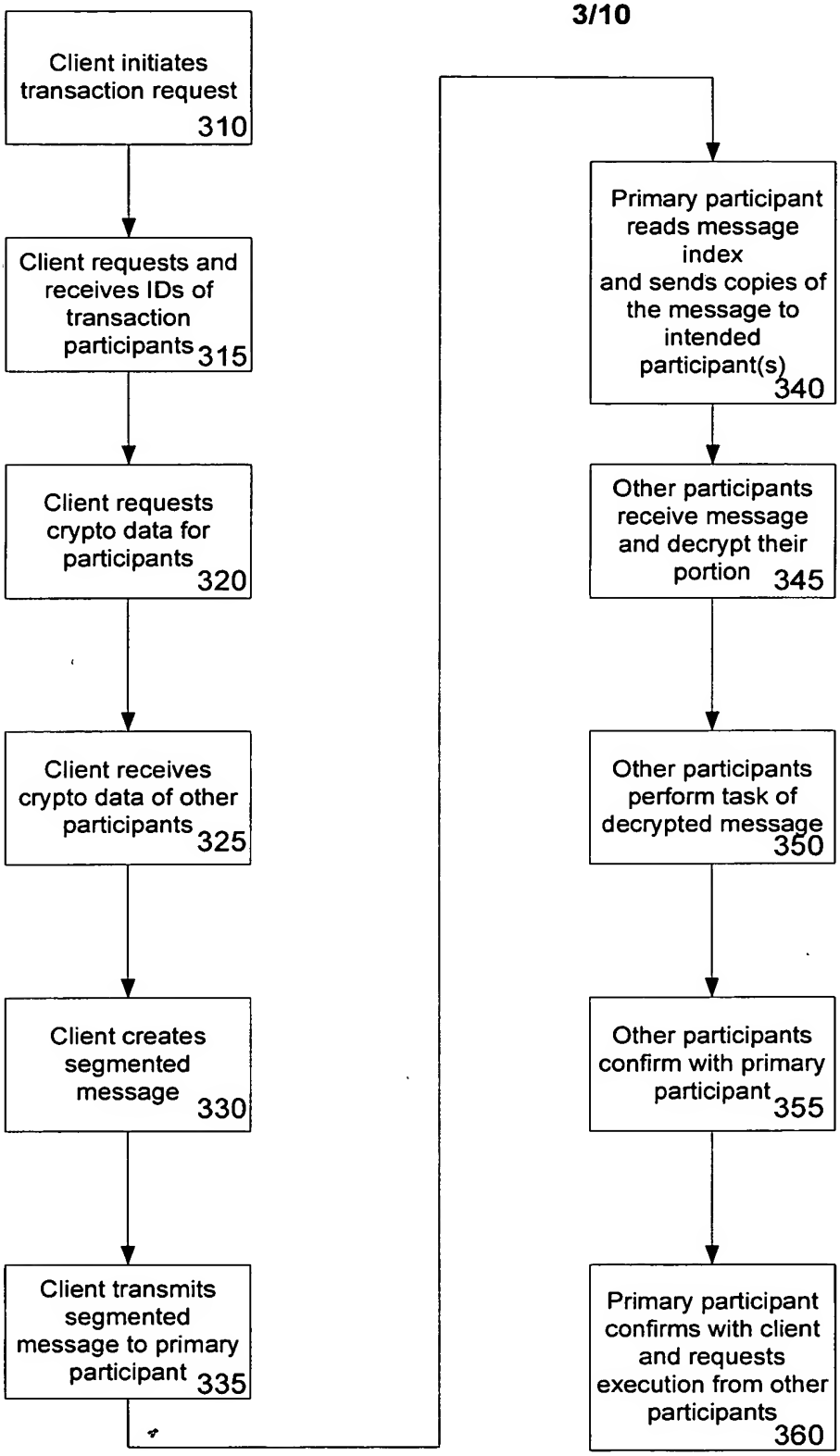
Client initiates transaction request 310
Client requests and receives IDs of transaction participants 315
Client requests crypto data for participants 320
Client receives crypto data of other participants 325
Client creates segmented message 330
Client transmits segmented message to primary participant 335
Primary participant reads message index and sends copies of the message to intended participant(s) 340
Other participants receive message and decrypt their portion 345
Other participants perform task of decrypted message 350
Other participants confirm with primary participant 355
Primary participant confirms with client and requests execution from other participants 360

Fig. 3

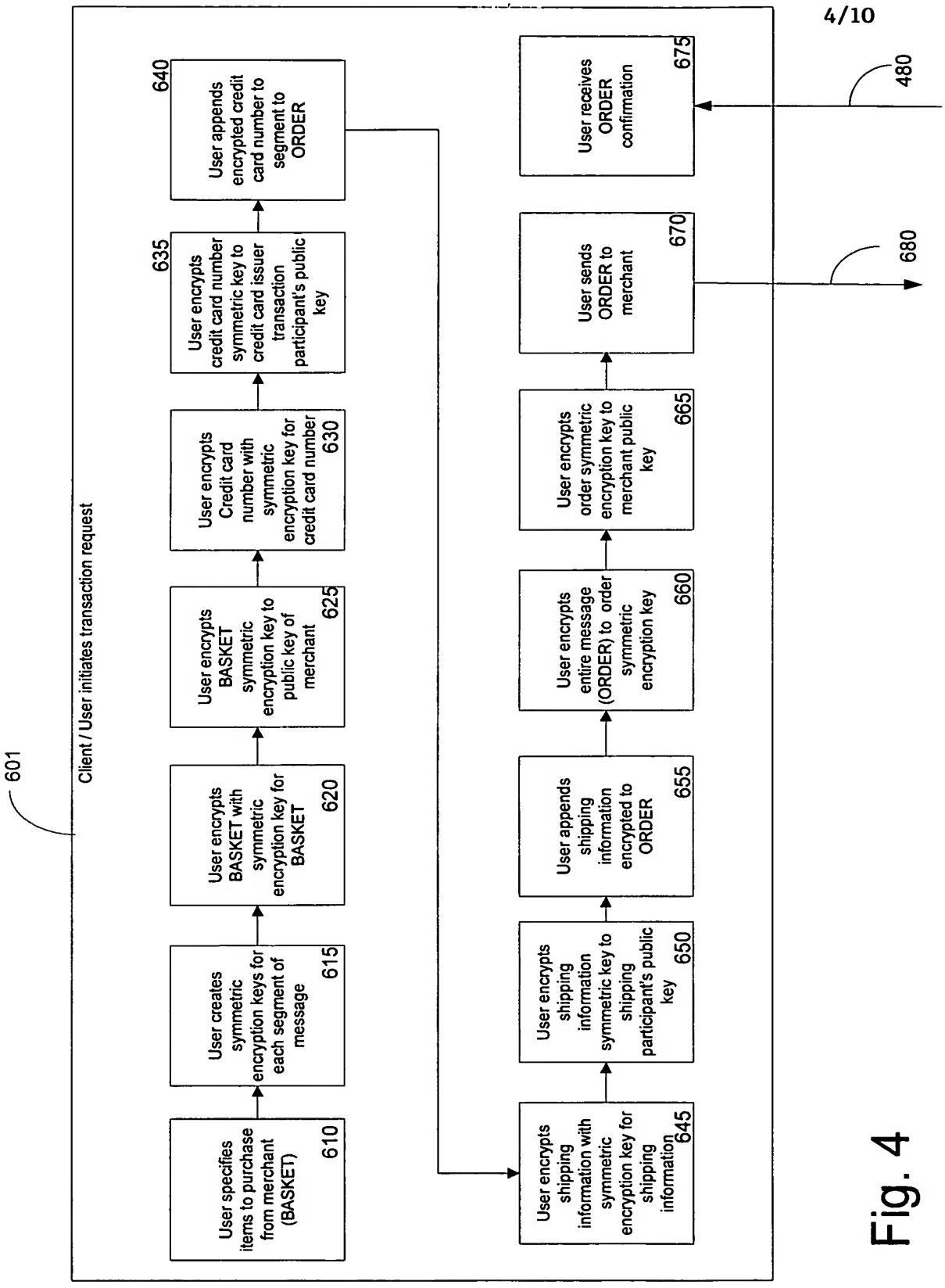
400
601
Client / User initiates transaction request
User specifies items to purchase from merchant (BASKET) 610
User creates symmetric encryption keys for each segment of message 615
User encrypts BASKET with symmetric encryption key for BASKET 620
User encrypts BASKET symmetric encryption key to public key of merchant 625
User encrypts Credit card number with symmetric encryption key for credit card number 630
User encrypts credit card number symmetric key to credit card issuer transaction participant's public key 635
User appends encrypted credit card number to segment to ORDER 640
User encrypts shipping information with symmetric encryption key for shipping information 645
User encrypts shipping information symmetric key to shipping participant's public key 650
User appends shipping information encrypted to ORDER 655
User encrypts entire message (ORDER) to order symmetric encryption key 660
User encrypts order symmetric encryption key to merchant public key 665
User sends ORDER to merchant 670
User receives ORDER confirmation 675
480
680

Fig. 4

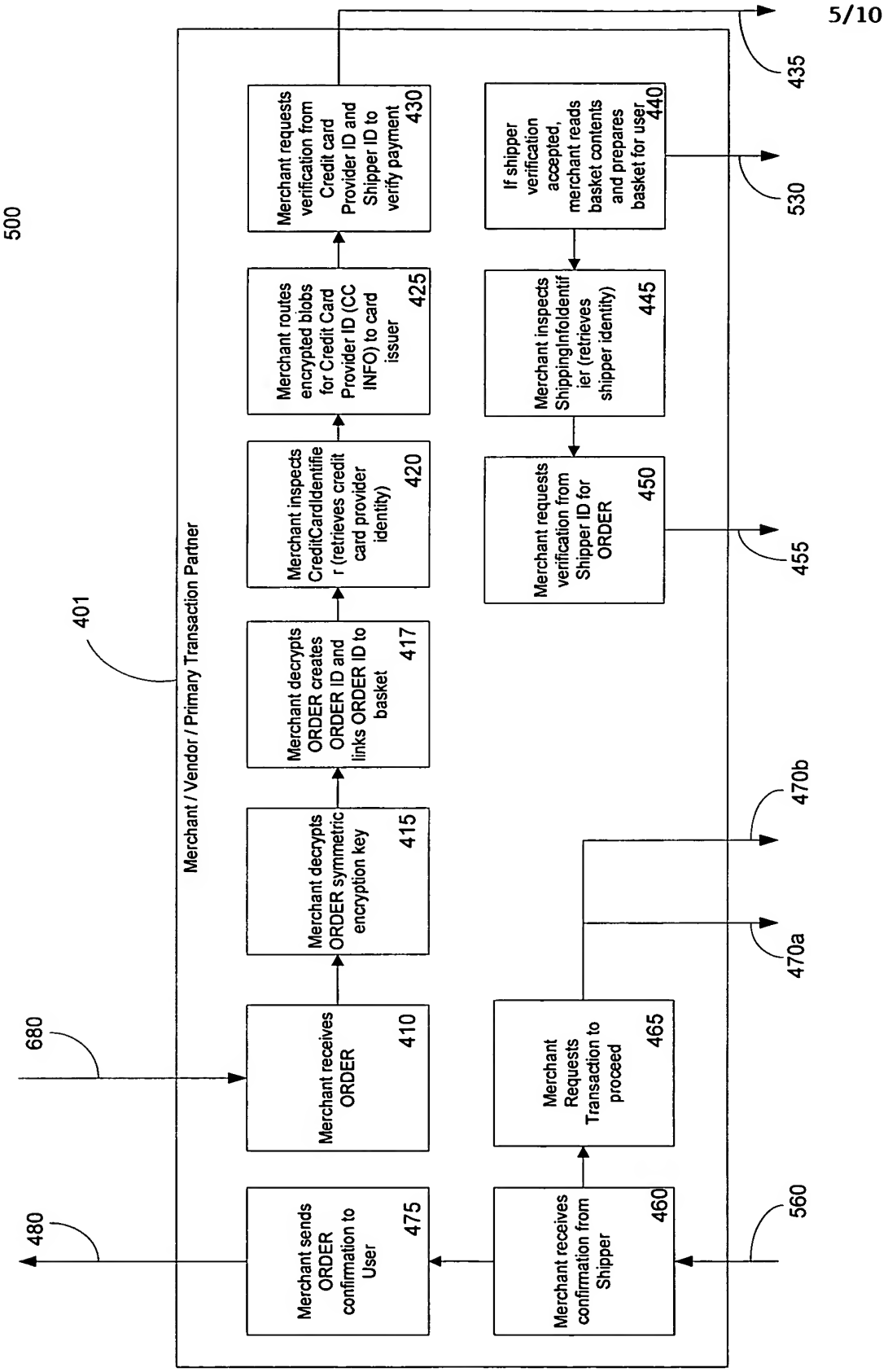
500
401
Merchant / Vendor / Primary Transaction Partner
680
480
560
530
435
455
470b
470a
Merchant receives ORDER 410
Merchant decrypts ORDER symmetric encryption key 415
Merchant decrypts ORDER creates ORDER ID and links ORDER ID to basket 417
Merchant inspects CreditCardIdentifier (retrieves credit card provider identity) 420
Merchant routes encrypted blobs for Credit Card Provider ID (CC INFO) to card issuer 425
Merchant requests verification from Credit card Provider ID and Shipper ID to verify payment 430
Merchant sends ORDER confirmation to User 475
Merchant receives confirmation from Shipper 460
Merchant Requests Transaction to proceed 465
Merchant requests verification from Shipper ID for ORDER 450
Merchant inspects ShippingInfoIdentifier (retrieves shipper identity) 445
If shipper verification accepted, merchant reads basket contents and prepares basket for user 440

Fig. 5

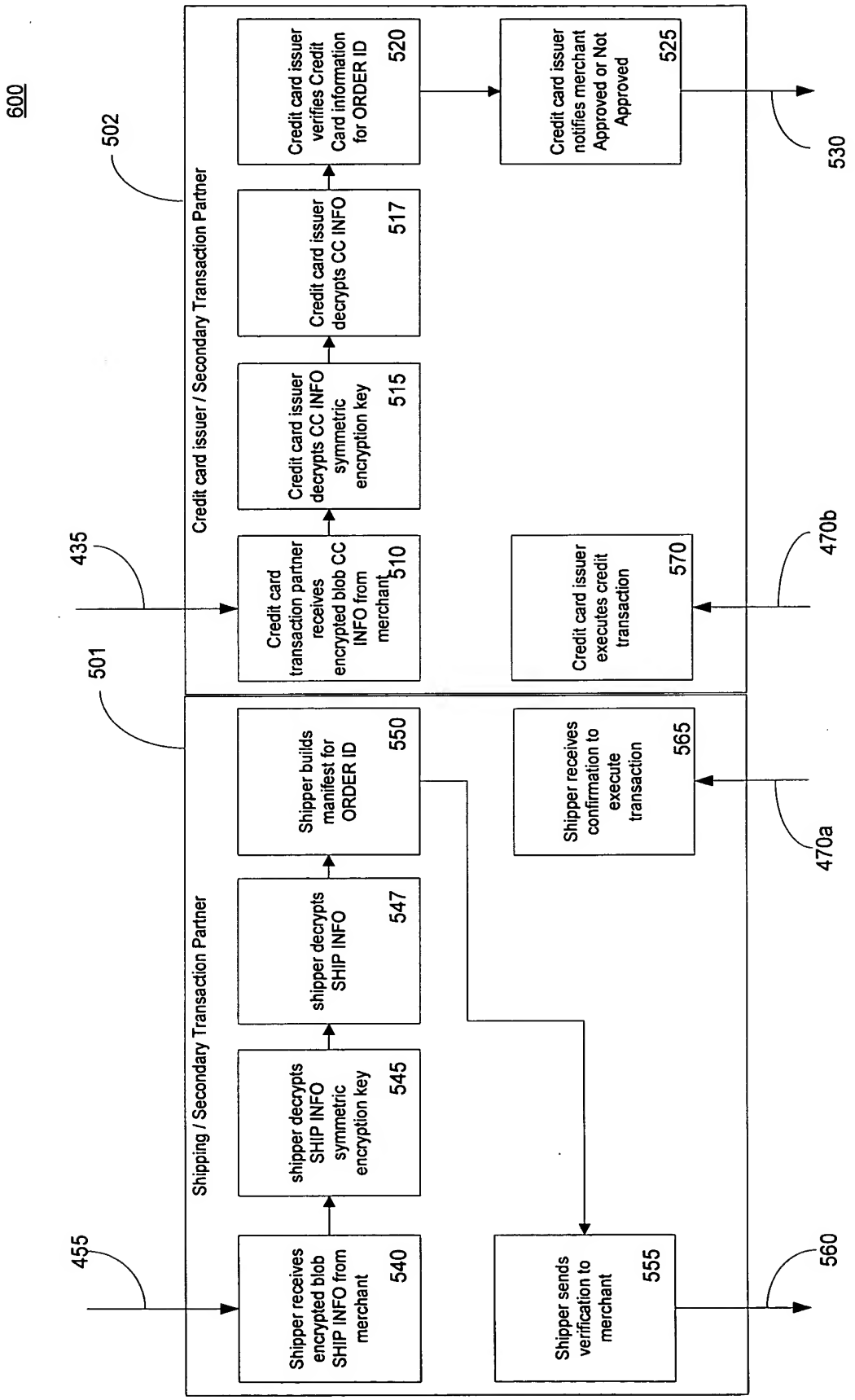
600
502
Credit card issuer / Secondary Transaction Partner
Credit card issuer verifies Credit Card information for ORDER ID 520
Credit card issuer notifies merchant Approved or Not Approved 525
530
Credit card issuer decrypts CC INFO 517
Credit card issuer decrypts CC INFO symmetric encryption key 515
435
Credit card transaction partner receives encrypted blob CC INFO from merchant 510
Credit card issuer executes credit transaction 570
470b
501
Shipping / Secondary Transaction Partner
Shipper builds manifest for ORDER ID 550
Shipper receives confirmation to execute transaction 565
470a
shipper decrypts SHIP INFO 547
shipper decrypts SHIP INFO symmetric encryption key 545
455
Shipper receives encrypted blob SHIP INFO from merchant 540
Shipper sends verification to merchant 555
560

Fig. 6

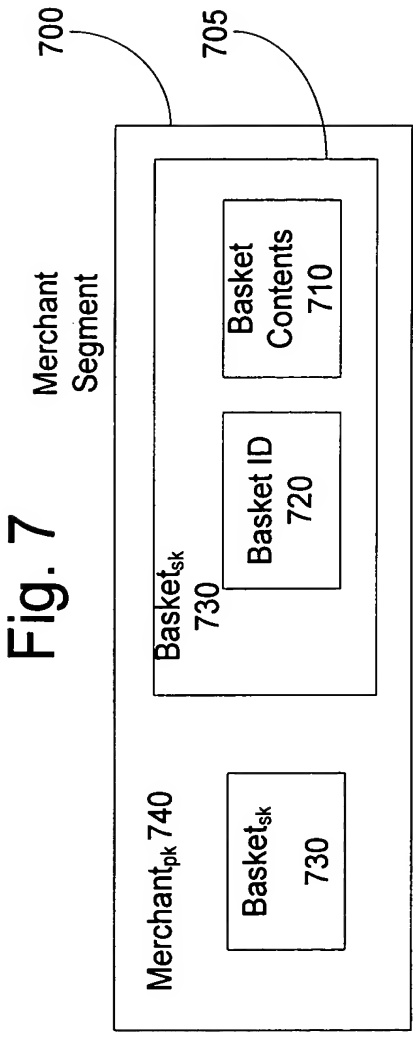
700
705
Merchant Segment
Basket Contents 710
Basket ID 720
Basket$_{sk}$ 730
Merchant$_{pk}$ 740
Basket$_{sk}$ 730

Fig. 7

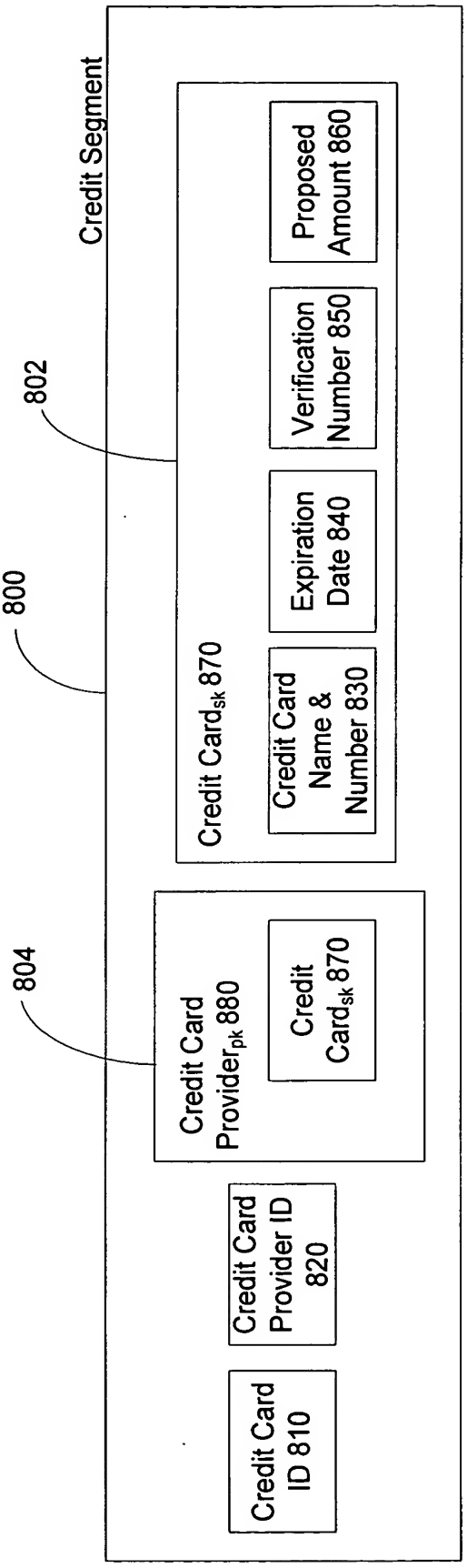
Credit Segment
802
800
804
Credit Card$_{sk}$ 870
Credit Card Name & Number 830
Expiration Date 840
Verification Number 850
Proposed Amount 860
Credit Card Provider$_{pk}$ 880
Credit Card$_{sk}$ 870
Credit Card Provider ID 820
Credit Card ID 810

Fig. 8

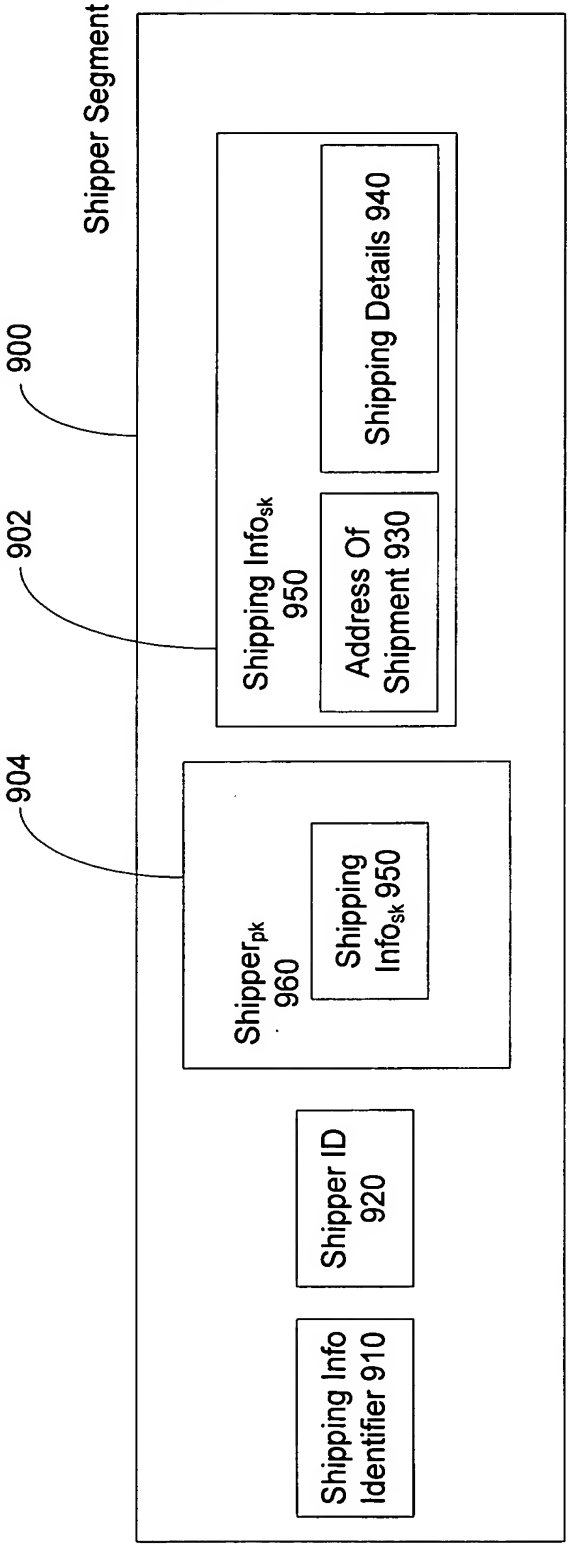
Shipper Segment
900
902
904
Shipping Info$_{sk}$ 950
Address Of Shipment 930
Shipping Details 940
Shipper$_{pk}$ 960
Shipping Info$_{sk}$ 950
Shipper ID 920
Shipping Info Identifier 910

Fig. 9

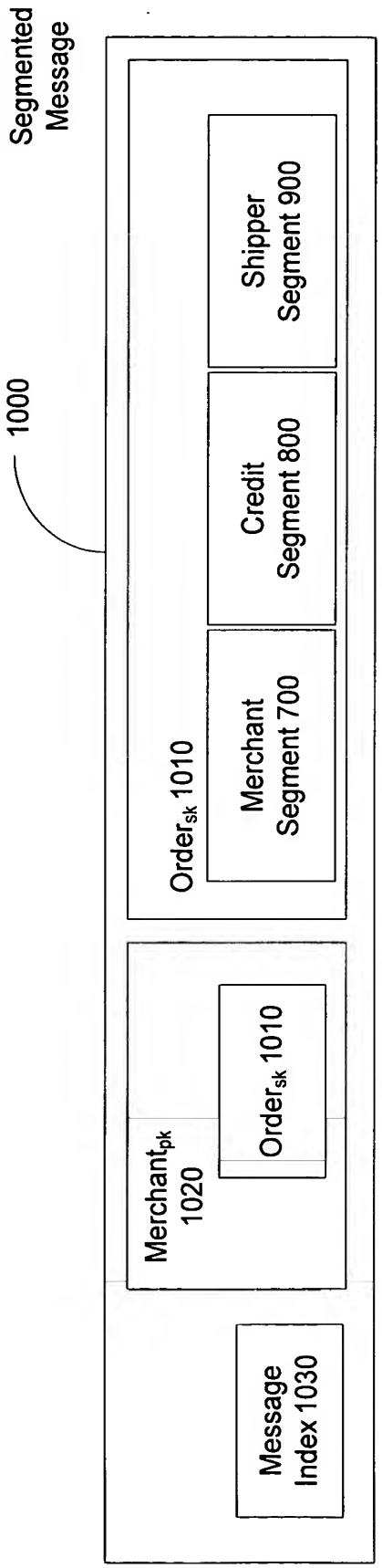
Segmented Message
1000
Order$_{sk}$ 1010
Merchant Segment 700
Credit Segment 800
Shipper Segment 900
Merchant$_{pk}$ 1020
Order$_{sk}$ 1010
Message Index 1030

Fig. 10

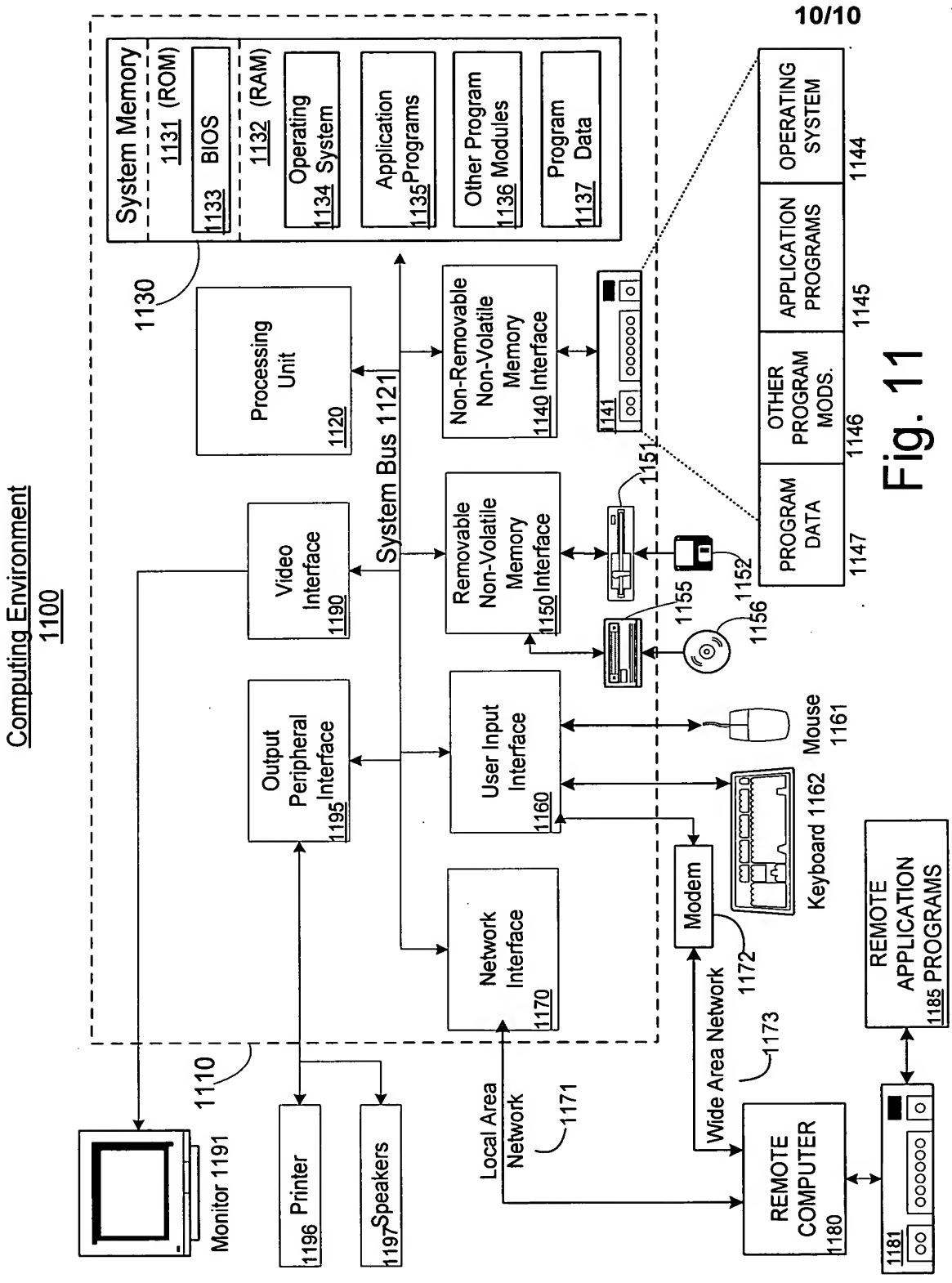
Computing Environment
1100
System Memory
1131 (ROM)
1133 BIOS
1132 (RAM)
Operating System 1134
Application Programs 1135
Other Program Modules 1136
Program Data 1137
1130
Processing Unit 1120
System Bus 1121
Non-Removable Non-Volatile Memory Interface 1140
Removable Non-Volatile Memory Interface 1150
Video Interface 1190
Output Peripheral Interface 1195
User Input Interface 1160
Network Interface 1170
Modem 1172
1110
Monitor 1191
Printer 1196
Speakers 1197
Local Area Network 1171
Wide Area Network 1173
Mouse 1161
Keyboard 1162
REMOTE COMPUTER 1180
REMOTE APPLICATION PROGRAMS 1185
1141
1151
1152
1155
1156
1181
OPERATING SYSTEM 1144
APPLICATION PROGRAMS 1145
OTHER PROGRAM MODS. 1146
PROGRAM DATA 1147

Fig. 11